NIST
National Institute of
Standards and Technology

INFORMATION
TECHNOLOGY
LABORATORY

Future USG Guidelines and Recommendations

Scott Rose, NIST

{scottr@nist.gov}

What's Next in DNSSEC

FOSE 2010, March 24th 2010

Cyber and Network Security Program

DNSSEC FISMA Controls in SP 800-53r3

- SC-20 (Authoritative side zone signing)
  - Applies to all levels
  - Does not differentiate between internal and external zones
  - Does not give explicit cryptographic guidance (that can be found in other NIST docs)
- SC-21 (Resolver side DNSSEC validation)
  - System must do validation when requested
  - Applies to HIGH Impact systems only
  - This is expected to change in future revisions (r4)

Other FISMA Controls for DNS/ DNSSEC

- SC-8: Transaction authentication
  - Mentioned DNS transactions, so options are:
    - TSIG/SIG(0)
    - Lower (network) level authentication (IPSec, etc.)
  - For MODERATE and HIGH Impact only
- SC-22: Provisioning
  - Non-DNSSEC security controls
    - Diverse secondaries
    - Platform hardening
    - etc…
  - For MODERATE and HIGH Impact only (now)
    - This may also change in future revisions (r4)

Crypto Guidance for USG

- SP 800-57 Part 1 & 3, and SP 800-81r1
  - *Note that the final 800-81r1 is different than the drafts!*
  - DNSSEC guidance slightly different than standard USG crypto guidance
    - Due to public nature of DNS (not just inter-USG communication)
    - Network issues with large DNS responses
    - Different Deadlines/phase out periods for algorithms and key lengths

Crypto Guidance: Key Size & Algorithm NIST SP 800-57 Part 1 & 3

- DNSKEY Algorithms
  - Should be migrating to RSA/SHA-256
  - RSA/SHA-1 will have to stick around for a while
    - For public validators which may not understand RSA/SHA-256 (dual signature algorithms in use?).
  - Migrate to ECDSA by 2015 (goal)
    - Not currently specified or implemented yet
- Key Lengths
  - 1024 bit ZSK's still acceptable until 2015
    - The firewall/router problem of large responses
  - KSK must be 2048 bits

Crypto Guidance: Key Lifetime NIST SP 800-81r1

- Largely unchanged
  - KSK: 1-2 years
  - ZSK: 1-3 months
- Local policy may favor shorter periods, but shouldn't favor longer
- No real hard requirements on signature lifetime
  - Obviously shorter than key lifetime (days/weeks)
  - SP 800-81r1 gives recommendations

What’s the deal with SHA-1?

- Phased out for inter-USG communications
  - Can’t for public, thus the dual use of RSA with SHA-1 and SHA-256 for a period of time
- SHA-1 still acceptable for some uses:
  - HMAC-SHA1 (used in TSIG)
    - if the shared secret string is random and long enough
  - DS and NSEC3 RR’s (hash not used for authentication, thus out of scope)
  - Wouldn’t hurt to do both (for DS RR’s) for a while as well and eventually migrate fully when it is safe to do so.

Resources

- NIST Guidance Docs at http://www.csrc.nist.gov
  - NIST SP 800-57 Parts 1 & 3
  - NIST SP 800-81r1
- NIST Testbed: Secure Naming Infrastructure Pilot (SNIP)
  - http://www.dnsops.gov/